Circuit arrangement with non-volatile memory module and method of en-/decrypting data in the non-volatile memory module

The present invention relates to a circuit arrangement for electronic data processing

- having at least one non-volatile memory module for storing data to be protected against unauthorized access by means of en-/decryption;
- having at least one memory module interface logic circuit assigned to the memory module
  -- for addressing the memory module,
  -- for writing the data to the memory module and
  -- for reading the data from the memory module;
- having at least one code R[ead]O[nly]M[emory] module for storing at least one R[ead]O[nly]M[emory] code; and
- having at least one code ROM module interface logic circuit assigned to the code ROM module
  -- for addressing the code ROM module and
  -- for reading the ROM code from the code ROM module.

The present invention further relates to a method of en-/decrypting data to be protected against unauthorized access in at least one non-volatile memory module.

Conventionally, key codes necessary for encrypting or decrypting the contents of a N[on]V[olatile] memory module are either hard-coded, defined by means of fuse cells especially instantiated therefor or saved themselves in a specially protected area of the non-volatile memory module.

Each of these known procedures has disadvantages, however: in the case of hard-coded keys, the key code cannot be changed for different controller versions with different ROM codes; in the case of the more flexible definition of the key code in fuse cells or in the case of protected E[lectrical] E[rasable] P[rogrammable] R[ead]O[nly]M[emory] areas, the key length is limited as a result of cell or surface area requirements.

Taking as basis the above-described disadvantages and shortcomings and acknowledging the outlined prior art, it is an object of the present invention so to develop a circuit arrangement of the above-mentioned type and an en-/decryption method of the above-

mentioned type based thereon that on the one hand the key code may be changed for different controller versions with different ROM codes and on the other hand the length of the key code is not limited.

This object is achieved with a circuit arrangement having the features indicated in claim 1 and by an en-/decryption method based thereon having the features indicated in claim 6. Advantageous embodiments and expedient further developments of the present invention are identified in the respective dependent claims.

According to the teaching of the present invention, therefore, a completely new approach is disclosed to the generation of at least one especially long key for the en-/decryption of at least one N[on]V[olatile] memory module from R[ead]O[nly]M[emory] code data, for example for embedded security controllers.

For this en-/decryption of the NV memory module, the key code is extracted from the ROM code available to the (micro-)controller, which ROM code is a constant from the point of view of the NV memory module; in this manner, a key code is generated which, with up to one byte of key per byte of plain/cipher text, may be described as relatively long.

According to a particularly inventive further development, the key (code) may be generated

- either by reading out the ROM code from the code ROM module in parallel with writing or reading of the non-volatile memory module
- or by one-off reading out of particular ROM code bytes at the time of the so-called "reset sequence" and by storing these ROM code bytes in at least one key register, until the ROM code bytes are required for at least one write operation or read operation of the NV memory module.

According to an advantageous development of the present invention, the quality of the key code may be further improved by supplementary or additional measures, such as for example by at least one additional address dependency or by scrambling by means of at least one scrambling logic circuit, which then counteracts the relatively regular structure of ROM codes.

The above-described invention is advantageously not limited methodologically to particular en-/decryption methods, but may be adapted with regard to key length and/or with regard to quality to the respective requirements of the method used.

Through double use of the ROM code as a source for long key codes, the security of the encryption or decryption of the N[on]V[olatile] memory module is increased

by greater key lengths, without such a greater key length resulting in a corresponding additional surface area requirement for storing this key code.

Furthermore, the person skilled in the art of cryptology will particularly appreciate the fact that the key codes generated according to the invention are dependent on the ROM code of the code ROM module, i.e. change with varying ROM codes.

The present invention further relates to a microcontroller, in particular an "embedded security controller", comprising at least one data processing device according to the above-described type. Accordingly, the above-described method may preferably be built into all smart card developments, for example.

The present invention finally relates to the use of at least one circuit arrangement of the above-described type in at least one chip unit, in particular in at least one "embedded security controller".

As already discussed above, there are various possible ways of advantageously embodying and developing the teaching of the present invention. Reference is made, in this regard, to the claims subordinate to claims 1 and 6, and the invention will be further described with reference to examples of embodiments shown in the drawings to which, however, the invention is not restricted. In the Figures:

Fig. 1 is a schematic block diagram of an example of embodiment of a circuit arrangement according to the present invention, by means of which the en-/decryption method may be performed according to the present invention.

Fig. 1 shows an example of embodiment of a circuit arrangement 100 for electronic data processing; in particular, the circuit arrangement 100 is provided for use in a microcontroller of the "embedded security controller" type.

This circuit arrangement 100 comprises a multi-component N[on]V[olatile] memory module 10, which takes the form of an E[lectrical] E[rasable] P[rogrammable]R[ead]O[nly]M[emory] and by means of which data may be stored which are to be protected from unauthorized access by encryption or decryption.

Assigned to this N[on]V[olatile] memory module 10 is a memory module interface logic circuit 12, by means of which

- the memory module 10 may be addressed (--> reference numeral 120a: address data "ADDR(a:0)" from the memory module interface logic circuit 12 to the memory module 10),

- the memory module 10 may be written to (--> reference numeral 120w: signal data "DIN(d:0)" from the memory module interface logic circuit 12 to the memory module 10) and

- the memory module 10 may be read out (--> reference numeral 120r: signal data "DOUT(d:0)" from the memory module 10 to the memory module interface logic circuit 12).

In addition, the circuit arrangement 100 comprises a code R[ead]O[nly]M[emory] module 20 for storing and supplying R[ead]O[nly]M[emory] codes. Assigned to this code ROM module 20 is code ROM module interface logic circuit 22, by means of which

- the code ROM module 20 may be addressed (--> reference numeral 220a: address data "A" from the code ROM module interface logic circuit 22 to the code ROM module 20) and

- the code ROM module 20 may be read out (--> reference numeral 220r: ROM code data or ROM code bytes "DO" from the code ROM module 20 to the code ROM module interface logic circuit 22).

The special feature of the circuit arrangement 100 according to Fig. 1 is that the key code for encrypting or decrypting the data assigned to the memory module 10 may be extracted and generated from the ROM code of the code ROM module 20.

To this end, the memory module interface logic circuit 12 comprises an en-/decryption logic circuit 14 having a key address generation unit 16 and a key register 18. The key address generation unit 16 is provided in this context for the purpose of generating an ROM key address (--> reference numeral 162a: ROM key address data from the key address generation unit 16 to a multiplexing unit 24 of the code ROM module interface logic circuit 22) in the case of write or read access to the memory module 10 using a memory module address coming from the C[entral]P[rocessing]U[nit] (--> reference numeral C12a: address data "CPU NV addr" from the CPU to the memory module interface logic circuit 12).

This multiplexing unit 24 integrated into the code ROM module interface logic circuit 22 receives not only an ROM key address of the key address generation unit 16, but also the address data coming from the CPU (--> reference numeral C22a: CPU ROM address

data "CPU ROM addr" from the CPU to the multiplexing unit 24 of the code ROM module interface logic circuit 22).

The ROM code is then fetched from the code ROM module 20 by means of the ROM key address and used as an en-/decryption key for encryption or decryption of

- the address data "CPU NV addr" from the CPU via the memory module interface logic circuit 12 to the memory module 10 (--> reference numeral C12a),

- the signal data "CPU NV write data" from the CPU via the memory module interface logic circuit 12 to the memory module 10 (--> reference numeral C12w) and

- the signal data "CPU NV read data" from the memory module 10 via the memory module interface logic circuit 12 to the CPU (--> reference numeral C12r).

The nub of the present invention is therefore that the circuit arrangement 100 according to Fig. 1 allows a method for encrypting or decrypting data to be protected against unauthorized access in the non-volatile memory module 10 to be performed, wherein the data assigned to the memory module 10 are encrypted or decrypted by means of the ROM code supplied by the code ROM module 20.

The quality of the key code generated may be further improved by scrambling by means of a scrambling logic circuit known per se (c.f. prior art DE 199 01 829 A1) but not shown explicitly in Fig. 1 for reasons of clarity, which then counteracts the relatively regular structure of the ROM code supplied by the code ROM module 20.

This scrambling logic circuit comprises

- a permutation stage for permuting bits of different value of the address signals "ADDR(a:0)" and/or data signals "DIN(d:0)" or "DOUT(d:0)" supplied to the scrambling logic circuit,

- an inversion stage for inverting the values of the bits of the address signals "ADDR(a:0)" and/or data signals "DIN(d:0)" or "DOUT(d:0)", wherein the permutation stage and the inversion stage are controlled by the scrambling pattern signals, and

- a decoding stage for obtaining control signals for the permutation stage and the inversion stage from the scrambling pattern signals.

With regard to generation of the key code serving in encryption or decryption, a distinction is drawn according to the present invention in principle between two variants (i) and (ii):

(i) generation of the key code in parallel with NV memory access, i.e. by reading out the ROM code in parallel with write/read access to the memory module 10:

Here, the en-/decryption logic circuit 14 in the respective interface (= memory module interface logic circuit 12) of the NV memory 10 obtains direct access to the unencrypted output data 220r of the code ROM module 20. In parallel with each write access (--> reference numeral 120w) to the NV memory 10 or with each read access (--> reference numeral 120r) to the page register of the NV memory 10, one byte of the ROM code is also read out from the code ROM module 20. The ROM code address 220a from which reading is performed is determined by the key address generation unit 16 of the en-/decryption logic circuit 14 but has to be unambiguous and reproducible for each NV memory address 120a.

For encryption (in the event of write access, reference numeral 120w) or decryption (in the event of read access, reference numeral 120r) of the NV memory data "DIN(d:0)" or "DOUT(d:0)", this ROM code byte is then used as a key byte or as part of the key byte, such that in an extreme case a key space is produced which is of exactly the same size as the code space of the N[on]V[olatile] memory module 10.

(ii) Generation of the key code in the reset phase, i.e. by one-off reading out of particular ROM code bytes, in particular at the time of the reset sequence, and by storing these ROM code bytes in the key register 18 until the time of a write/read access to the memory module 10, i.e. until these ROM code bytes are required for a write operation or a read operation of the memory module 10:

As a part of the "reset sequence" of the controller, a number of ROM code bytes are read out from the code ROM module 20 and stored in the key registers 18.

In the event of write or read access to the memory module 10, the content of these key registers 18 is used as the key or as parts of the key for encrypting or decrypting the NV memory data "DIN(d:0)" or "DOUT(d:0)" respectively.

LIST OF REFERENCE NUMERALS

100	Circuit arrangement for electronic data processing
10	N[on]V[olatile] memory module
12	Memory module interface logic circuit
14	En-/decryption logic circuit of the memory module interface logic circuit 12
16	Key address generation unit of the en-/decryption logic circuit 14
18	Key register of the en-/decryption logic circuit 14
20	Code R[ead]O[nly]M[emory] module
22	Code ROM module interface logic circuit
24	Multiplexing unit of the code ROM module interface logic circuit 22
120a	Address data "ADDR(a:0)" from the memory module interface logic circuit 12 to the memory module 10
120r	Signal data "DOUT(d:0)" from the memory module 10 to the memory module interface logic circuit 12
120w	Signal data "DIN(d:0)" from the memory module interface logic circuit 12 to the memory module 10
162a	ROM key address data from the key address generation unit 16 to the multiplexing unit 24
220a	Address data "A" from the multiplexing unit 24 to the code ROM module 20
220r	ROM code data or ROM code bytes "DO" from the code ROM module 20 to the code ROM module interface logic circuit 22
C12a	Address data "CPU NV addr" from the CPU to the memory module interface logic circuit 12
C12r	Signal data "CPU NV read data" from the memory module interface logic circuit 12 to the CPU
C12w	Signal data "CPU NV write data" from the CPU to the memory module interface logic circuit 12

C22a CPU ROM address data "CPU ROM addr" from the CPU to the multiplexing unit 24

C22r ROM code data "CPU ROM read data" from the code ROM module 20 to the CPU